COMMONWEALTH TELECOMMUNICATIONS ORGANISATION

Governance of cyberspace

A clash of values

By **Marcel Ambiana Belingue**, Head of Membership and Communications, Commonwealth Telecommunications Organisation, United Kingdom

We have entered highly promising times in our political, economic and social development; we are hovered up into fast-growing cyberspace where space and time are becoming almost immaterial and opportunities are being equalised for all. Ever more of us are empowered to share, trade, or meet and exchange with many others almost anywhere in the world, at the speed of light, thanks to information and communication technologies (ICTs). There is still some way to go before we achieve global access to ICTs, but in this seemingly borderless cyberspace, we reach out to anyone instantly and our ability to influence events nearer or further away from us seems almost without limitations. We even take collective action into cyberspace, and soon perhaps we will be able to 'tweet' into power (or 'flickr' out) entire governments. Boundaries between the physical and the virtual have blurred considerably, and such is the promise of cyberspace that it seems as if for many it has become a permanent space, a world of infinite possibilities.

At the same time, perhaps because of the growth and complexity of crime in cyberspace, the international community is yet to agree on if, and how the Internet, its main platform should be governed. Indeed, while the private sector embraces cyberspace and is able to adjust quickly to the opportunities and threats it brings, things are – yet again – proving too fast for notoriously slow governments that are struggling to agree on rules that should govern life in cyberspace at national and international levels.

Two opposing views continue to dominate the debate on the governance of the Internet: cyberspace ultraliberals' view that cyberspace should be immune from rules, state or corporate control, with anonymous communications, and cyberspace sceptics' view that rules and control should apply to address issues such as safety and crime in cyberspace. Opportunities in cyberspace continue to grow, but so are threats to individuals and organisations, and so consensus should be about finding the right balance between liberals and sceptics. We are constantly and increasingly exposed to, and are often also direct, indirect or collective victims of crimes of different kinds and scales: cyber-scams, cyber-thefts, cyber-bullying, hacking, phishing, spamming, cyber-terrorism, cyber-warfare, and cyber-attacks (including DDoS, or distributed denial of service attacks, as reported in a cyber 'stand-off' during the escalating crisis between Ukraine and Russia over Crimea).

While international consensus has been reached on other previously contentious Internet issues and action is being taken in areas such as cybersecurity and cybercrime, 'blocs' have emerged over who should govern the Internet,

COMMONWEALTH TELECOMMUNICATIONS ORGANISATION

CORE VALUES IN THE 2013 COMMONWEALTH CHARTER

1. Democracy
2. Human rights
3. International peace, security and economic development
4. Tolerance, respect and understanding
5. Freedom of expression
6. Rule of law
7. Good governance
8. Sustainable development
9. Protecting the environment
10. Access to health, education, food and shelter
11. Gender equality
12. Importance of young people in the commonwealth
13. Recognition of the needs of small states
14. Recognition of the needs of vulnerable states
15. The role of civil society
16. Cyberspace itself

with rather unexpected alliances. The last World Conference on International Telecommunications (WCIT) organised by the International Telecommunication Union (ITU) in Dubai in December 2012 opposed pro- and anti-ITU countries who sought but could not reach a consensus on the inclusion of the Internet within international telecommunications regulations (ITRs) and thus, a role or not for the ITU in the Internet space; in the closing hours of the 12-day event, Iran's call for a formal vote – instead of a consensus – on a specific human rights language proposed to be included in the new ITR treaty unexpectedly favoured US and other countries such as the UK, Japan and Australia opposed to using the UN framework to govern the Internet, effectively postponing the much needed broader international consensus WCIT was expected to secure on the governance of the Internet.

While the Dubai WCIT was seen as a success by the ITU's leadership, anti-UN control observers described it as a mere failed UN attempt to take over the Internet. More ironically, for others, WCIT was primarily about pro-human rights countries claiming a right to use denial of access to the Internet against target anti-human rights countries, while those considered anti-human rights were the ones insisting on universal access to the Internet.

Five months after the Dubai WCIT, whistleblower Edward Snowden's release of documents detailing large scale global surveillance activities by the US and the UK will come to discredit them significantly as pro-human rights and anti-UN control countries.

The current divide is not surprising. It mirrors real international differences over how to balance security, safety, privacy and freedom of expression that already exist offline or, put simply, differences over what should be allowed or prohibited online, and who should control the Internet.

For some, the Dubai WCIT outcome is indicative of the lack of understanding of what the Internet is. As most "unowned" technologies, the Internet grew primarily out of consensus among all actors – how to make it work for all and how to resolve disputes, and consensus remains the best way to guarantee its further development, argues Jonathan Zittrain, professor of law and professor of computer science at Harvard University.

In March 2014, Commonwealth countries adopted a cyber-governance model based on the key idea that what is unacceptable offline is unacceptable online. The model builds on the core values promoted in the Charter of the Commonwealth and provides a guide in which governments, industry, civil society and users all have a shared responsibility in tackling cyber-threats to society.

Through this model, the 53-group of countries have resolved to uphold the core values included in the Charter, but also to engage in collaboration and mutual support. Member countries will be guided by four key principles:

- They contribute to a safe and an effective global cyberspace
- Their actions in cyberspace support broader economic and social development
- They act individually and collectively to tackle cybercrime
- They each exercise their rights and meet their responsibilities in cyberspace.

Commonwealth cyber governance principles and suggested actions are provided on pages 56 and 57, and the full model can be downloaded at http://www.cto.int/focus-themes/cybersecurity

Far from a wasted effort, WCIT has at least allowed for the most open international debate to date on the governance of the Internet. But, as a voluntary association of independent countries, the Commonwealth clearly offers its members greater scope for a consensual rather than a prescriptive Internet future. In addition, its model is not limited to the Internet but covers, more widely, cyberspace. Hopefully, NETmundial, the Brazil-hosted global consultation taking place this month in Sao Paulo on the future of the Internet will reflect on this approach to help find a way forward, be it within or outside of the UN framework.